VMM & UM in Incident Response

Boris Parák\textsuperscript{1} \hspace{1cm} Slávek Licehammer\textsuperscript{1,2}

\textsuperscript{1}CESNET

\textsuperscript{2}Masaryk University

May 20, 2015
User Management
User Suspension
User Suspension

Perun

VO

Facility

Site

VO

Facility

Site

VO

Facility

Site

VOMS

Argus
User Suspension
Virtual Machine Management
Complaint containing an IP address

- tool to pair the address in question with an NGI/a SITE
- notify the NGI/SITE and let them handle it

Proposed:

- GOCDB has a field for IP ranges (multiple, comma-separated)
- SITEs need to fill this in ASAP, all of them
- proof-of-concept script taking an IP address and outputting the name and contact for NGI/SITE
Appliance in AppDB is vulnerable

- tool to locate all SITEs deploying this appliance
- mark this appliance/image as suspended in AppDB
- notify NGIs/SITEs and let them handle it (running)

Proposed:

- AppDB provides information about subscribed SITEs
- proof-of-concept script taking MPURI and outputting a list of NGIs/SITEs
- AppDB suspension?
Compromised user account/credentials

⇝ User Management
Complaint containing an IP address

- locate the virtual machine by IP address
- trigger established IR procedures
- report to EGI CSIRT with details (owner, analysis)

Proposed:

- proof-of-concept script taking an IP address, CMF specific
- need clear (amended) procedures for incident handling in the cloud
- list of required information for VMM IR, \( \rightsquigarrow \) EGI CSIRT
Appliance in AppDB is vulnerable

- locate virtual machine(s) by appliance MPURI (disk/image)
- trigger established IR procedures
- report to EGI CSIRT with details (owner, analysis)

Proposed:

- proof-of-concept script taking an MPURI, CMF specific
- need clear (amended) procedures for incident handling in the cloud
- list of required information for VMM IR, ~ EGI CSIRT
- Warn users running instances of this appliance?
User is reported/compromised

⇒ EGI CSIRT ⇒ User Management
IR Procedure(s)
Discussion

(What? When? Where? How?)

• carefully analyze and observe from the outside
• create a permanent copy without disrupting (snapshot?)
• attempt to enter the instance if possible and gather data
• suspend by creating a memory snapshot
• explore flow monitoring logs
• locate similar running instances/appliances
• report upstream for global action